



FIGURE 1

TI3C1D9814IBYE5IDIC0A802FFIDP8AIDU0IEP800IPK1IPR11ISIC0A80263ISP8A
TI3C1D9821IBY5CIDIC0A80215IDU3CIEP806IPK2ISA0000E8DA99DCISIC0A80201
TI3C1D9834IBY4EIDIC0A802FFIDP89IDU0IEP800IPK1IPR11ISIC0A80297ISP89
TI3C1D9839IBY114IDU3AIEP1FIPK6
TI3C1D9878IBYA6IDU0IEPA6IPK1
TI3C1D9878IBYE5IDIC0A802FFIDP8AIDU0IEP800IPK1IPR11ISIC0A80297ISP8A
TI3C1D987EIBY114IDU3AIEP1FIPK6
TI3C1D988EIBY148IDIC0A80219IDP43IDU0IEP800IPK1IPR11ISIC0A80299ISP44
TI3C1D988EIBY148IDIC0A80299IDP44IDU0IEP800IPK1IPR11ISIC0A80219ISP43
TI3C1D988EIBY2EIDIC0A80219IDU0IEP806IPK1ISA009027078E8EISIC0A80299

FIGURE 2



---Timestamp
TI-start-time in seconds (since 1970 GMT)
DU-duration of validity (for time grouping)

---Structural Fields
GB-indicator that this row is an output of grouping operation
MP-indicator that this row is a mapping or lookup row

---Key Fields (this category includes Secondary Key Fields):
CD-collection device (i.e. origin of the data)
DA-destination MAC address (as stated by ARP packet)
DD-destination domain (DNS style)
DI-destination IP number

DM-destination MAC address (true MAC address)
DN-normalised destination address
DP-destination TCP port or UDP port
EP-Ethernet protocol number
PR-IP protocol number
SA-source MAC address (as stated by ARP packet)
SD-source domain (DNS style)
SI-source IP number
SM-source MAC address (true MAC address)
SN-normalised source address
SP-source TCP port or UDP port

---Secondary Key Fields (actually, special case of Key Fields)
TF-traffic flow
AC-account category
SA-sub-account category
CC-cost centre category

---Counter fields
BY-count of bytes
PK-count of packets
HT-count of web hits

FIGURE 3